UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22850 7590 03/18/2011
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LE, CANH	
ART UNIT	PAPER NUMBER
2439	

DATE MAILED: 03/18/2011

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841

TITLE OF INVENTION: ENCRYPTION PROCESSING APPARATUS AND ENCRYPTION PROCESSING METHOD FOR SETTING A MIXED ENCRYPTION PROCESSING SEQUENCE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	06/20/2011

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22850 7590 03/18/2011

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841

TITLE OF INVENTION: ENCRYPTION PROCESSING APPARATUS AND ENCRYPTION PROCESSING METHOD FOR SETTING A MIXED ENCRYPTION PROCESSING SEQUENCE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	06/20/2011

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, CANH	2439	713-189000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 ______________________
2 ______________________
3 ______________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee
□ Publication Fee (No small entity discount permitted)
□ Advance Order - # of Copies ______________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.
□ Payment by credit card. Form PTO-2038 is attached.
□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number __________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ______________________ Date ______________________

Typed or printed name ______________________ Registration No. ______________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841

22850 7590 03/18/2011
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LE, CANH	
ART UNIT	PAPER NUMBER
2439	

DATE MAILED: 03/18/2011

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 864 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 864 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 10/749,412	**Applicant(s)** OCHI ET AL.	
	Examiner CANH LE	**Art Unit** 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/16/2010*.

2. ☒ The allowed claim(s) is/are *1,3-6,8,9,11,13-16,18,19 and 21-23*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☒ All b) ☐ Some* c) ☐ None of the:

   1. ☒ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Canh Le/
Examiner, Art Unit 2439

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Sameer Gokhale on Tuesday March 8, 2011.

The newly amended set of claims as authorized by Applicant immediately follow:

Claim 1 (Currently Amended): An encryption processing apparatus configured to perform a data encryption process, said encryption processing apparatus comprising:

a processor configured to provide:

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device,

wherein each group includes a triple-DES encryption process and said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for an encryption processing sequence in at least one of said groups, and set the number of dummy single-DES processes to be a multiple of 3, and

said control section is configured to set a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and set one mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing the dummy encryption processing unit.

Claim 2 (Currently Canceled).

Claim 3 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said control section is configured to determine a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into the plurality of groups, and perform a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit.

Claim 4 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said encryption processing unit is a single-DES encryption process, and

wherein said control section is configured to set the mixed encryption processing sequence by dividing the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes and by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed.

Claim 5 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said control section is configured to perform a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units by using a single-DES encryption process which forms a triple-DES encryption process as an encryption processing unit.

Claim 6 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a random-number generation process, and

said control section is configured to form a random-number generation process as a process including a conversion process by three single-DES processes, and sets the three single-DES processes as a random-number generation process in one of the groups of divisions.

Claim 7 (Canceled).

Claim 8 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein said encryption processing apparatus has a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence set by said control section, and

said control section is configured to store the processing results in said memory to identify which encryption processing unit the processing results are obtained from.

Claim 9 (Currently Amended): An encryption processing apparatus configured to perform a data encryption process, said encryption processing apparatus comprising:

a processor configured to provide:

a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second one of the groups and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section adding dummy encryption processing units as encryption processing units to at least one of the groups that performs dummy encryption processes that are unnecessary for the original encryption processing sequence, and said control section performing a mixing of processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device,

wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process, said control section is configured to set said dummy encryption processes as single-DES encryption processes and

wherein said control section is configured to set the number of dummy encryption processes to a multiple of 3.

Claim 10 (Currently Canceled).

Claim 11 (Currently Amended): An encryption processing method, implemented on an encryption processing apparatus, for performing a data encryption process, said encryption processing method comprising:

dividing, at the encryption processing apparatus, an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group;

setting, at the encryption processing apparatus, a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from another the second group and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed; and

performing, at the encryption processing apparatus, an encryption process in accordance with the mixed encryption processing sequence set in said setting; and

transmitting, from the encryption processing apparatus, each of encrypted output data generated independently by the first group and the second group to an external device,

wherein each group includes a triple-DES encryption process and said dividing includes setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3, said method further comprising:

setting a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and

setting the mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing unit.

Claim 12 (Currently Canceled).

Claim 13 (Previously Presented): The encryption processing method according to Claim 11, wherein said dividing determines a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into the plurality of groups, and performs a process for setting a group of divisions in which each of the sequences in the group of sequences can be performed independently as a unit.

Claim 14 (Previously Presented): The encryption processing method according to Claim 11, wherein each of said encryption processing units is a single-DES encryption process,

said dividing divides the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes, and

said setting sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed.

Claim 15 (Previously Presented): The encryption processing method according to Claim 11, wherein said dividing performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with a single-DES encryption process which forms a triple-DES encryption process being an encryption processing unit.

Claim 16 (Previously Presented): The encryption processing method according to Claim 11, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a random-number generation process, and

said encryption processing method further comprises forming a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random-number generation process in one of the groups.

Claim 17 (Canceled).

Claim 18 (Previously Presented): The encryption processing method according to Claim 11, further comprising:

storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence to identify which encryption processing unit the processing results are obtained from.

Claim 19 (Currently Amended): An encryption processing method, implemented on an encryption processing apparatus, for performing a data encryption process, said encryption processing method comprising:

dividing, at the encryption processing apparatus, an original encryption processing sequence, into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group,

setting, at the encryption processing apparatus, a mixed encryption processing sequence by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group;

performing, at the encryption processing apparatus, an encryption process in accordance with said mixed encryption processing sequence; and transmitting, from the encryption processing apparatus, each of encrypted output data generated independently by the first group and the second group to an external device,

wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said setting sets said dummy encryption processes as a single-DES encryption process, and

wherein said dividing includes setting the number of dummy encryption processes to a multiple of 3.

Claim 20 (Currently Canceled).

Claim 21 (Currently Amended): A non-transitory computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method comprising:

dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group;

setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units, set in said dividing, within each group is fixed;

performing an encryption process in accordance with the mixed encryption processing sequence set in said setting; and

transmitting each of encrypted output data generated independently by the first group and the second group to an external device,

wherein each group includes a triple-DES encryption process and said dividing includes setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3, said method further comprising:

setting a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and

setting the mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing unit.

Claim 22 (Currently Amended): A non-transitory computer readable storage medium encoded with computer executable instructions, which when executed by a computer, cause the computer to perform a method comprising:

dividing an original encryption processing sequence, into a plurality of groups which each include a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group;

setting a mixed encryption processing sequence by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence and by mixing processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group; and

performing an encryption process in accordance with said mixed encryption processing sequence; and

transmitting each of encrypted output data generated independently by the first group and the second group to an external device, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said setting sets said dummy encryption processes as a single-DES encryption process, and

wherein said dividing includes setting the number of dummy encryption processes to a multiple of 3.

Claim 23 (Previously Presented): The encryption processing apparatus according to Claim 1, wherein the first input data to be encrypted for the first group is received from the external device, the second input data to be encrypted for the second group is a random number generated at the encryption processing apparatus, and each of encrypted output data generated independently by the first group and the second group that is sent to the external device is used to verify that the encryption processing apparatus and the external device share a valid common key.

DETAILED ACTION

This Office Action is in response to the application filed on 12/16/2010.

Claims 1, 3-6, 8-11, 13-16, and 18-23 have been pending.

Reasons for Allowance

Claims 1, 3-6, 8-9, 11, 13-16, 18-19, and 21-23 are allowed.

The following is an examiner's statement for reasons for allowance:

The prior art of record, either singularly or in combination, failed to teach the combination of the invention as claimed in independent claims 1, 11, and 21. For example, it failed to teach "a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second group of the groups, and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group and under a condition in which a processing sequence of the encryption processing units within each of the plurality of groups is fixed;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device,

wherein each group includes a triple-DES encryption process and said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for an encryption processing sequence in at least one of said groups, and set the number of dummy single-DES processes to be a multiple of 3, and

said control section is configured to set a dummy encryption processing unit that performs the dummy encryption process in at least one of the groups, and set one mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing the dummy encryption processing unit."

The prior art of record, either singularly or in combination, failed to teach the combination of the invention as claimed in independent claims 9, 19, and 22. For example, it failed to teach "a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups, each group being composed of a plurality of encryption processing units, each encryption processing unit being a defined process, each group being a separate and independent encryption process for encrypting an input data, where a first input data to be encrypted for a first group of the groups is different relative to a second input data to be encrypted for a second one of the groups and the first input data to be encrypted for the first group is generated independently relative to the second input data to be encrypted for the second group, said control section adding dummy encryption processing units as encryption processing units to at least one of the groups that performs dummy encryption processes that are unnecessary for the original encryption processing sequence, and said control section performing a mixing of processing sequences of the encryption processing units of the plurality of groups with each other by executing performance of at least one encryption processing unit from the first group at a time between executing performance of encryption processing units from the second group;

an encryption processing section configured to perform an encryption process in accordance with the mixed encryption processing sequence set by said control section; and

a transmitting unit configured to transmit each of encrypted output data generated independently by the first group and the second group to an external device,

wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process,

said control section is configured to set said dummy encryption processes as single-DES encryption processes and

wherein said control section is configured to set the number of dummy encryption processes to a multiple of 3."

Claims 3-6 and 8 depend on claim 1, and are therefore considered as allowable claims.

Claims 13-16, 18, and 23 depend on claim 11, and are therefore considered as allowable claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

March 11, 2011

/Christopher J Brown/
Primary Examiner, Art Unit 2439